

# AirTight WIPS

The Only True Wireless Intrusion Prevention System



# Undisputed Global Leader in Wireless Security

- AirTight invented wireless intrusion prevention; owns 29 granted patents

## Gartner on AirTight

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirTight Networks					x
Aruba Networks				x	
Cisco				x	
Fluke Networks				x	
Meraki		x			
Motorola				x	

## AirTight WIPS is the only WIPS:

- Ever to receive the highest “Strong Positive” rating from Gartner – now two years in a row!
- Rated at the top by Gartner in all its six MarketScope reports on WLAN IPS

## US DoD Approved



## AirTight WIPS is the only WIPS:

- Certified for Common Criteria EAL2+, FIPS 140-2 and DISA UC APL

# Trusted by Thousands of Customers Worldwide

## Government



## Telco



## Manufacturing



## Technology



## Transportation



## Financial



## Services



## Retail



## Hospitality



## Healthcare





# Wireless Security



# (Re)Considering Wireless Security

## What does not work?

A “No Wi-Fi” policy without enforcement



We don't have “that” problem because...



# TJX Breach – The Tip of the Iceberg

## THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

### TJX Hacker Charged With Heartland, Hannaford Breaches

By Kim Zetter  August 17, 2009 | 2:34 pm | Categories: Breaches

The constellation of hacks connected to the TJX hacker is growing.

Albert "Segvec" Gonzalez has been indicted by a federal grand jury in New Jersey — along with two unnamed Russian conspirators — on charges of hacking into Heartland Payment Systems, the New Jersey-based card processing company, as well as Hannaford Brothers, 7-Eleven and two unnamed national retailers, according to the indictment unsealed Monday. Gonzalez, a former Secret Service informant, is already awaiting trial over his involvement in the TJX hack.

According to the court document, the [hackers allegedly stole more than 130 million credit and debit card numbers](#) (.pdf) from Heartland and Hannaford combined. Prosecutors say they believe these breaches constitute the largest data-breach and identity-theft case ever prosecuted in the United States. They're investigating other breaches and have not ruled out Gonzalez's involvement in even more intrusions.



## Additional breaches

**Marshalls.**

**SPORTS AUTHORITY.**

 **Heartland**  
PAYMENT SYSTEMS



 **OfficeMax**®

**BARNES & NOBLE**  
BOOKSELLERS

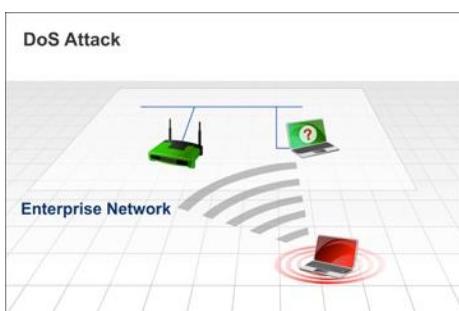
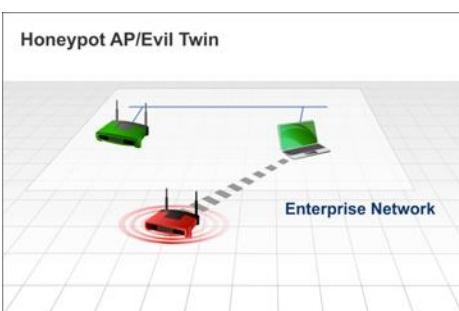
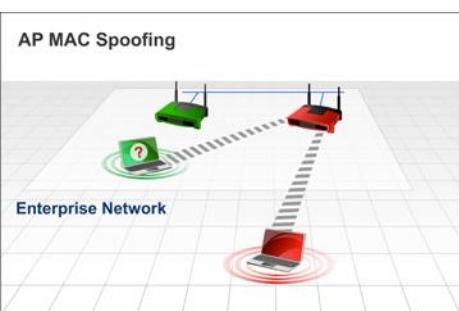
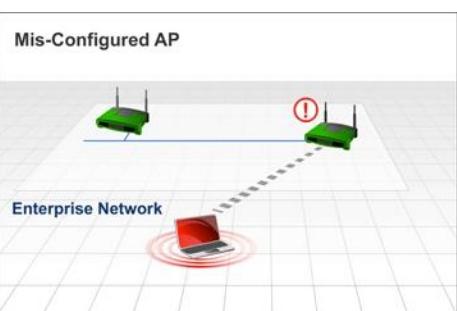
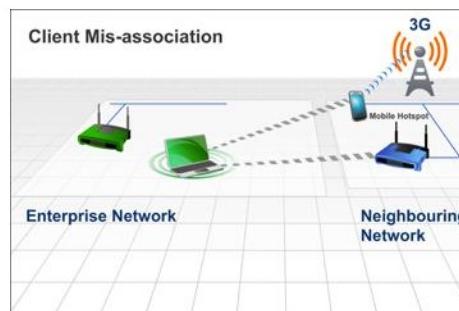
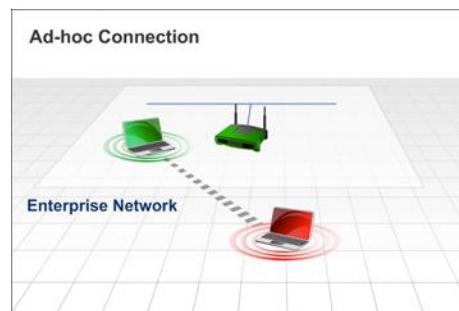
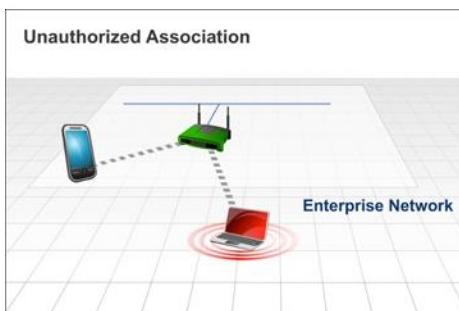
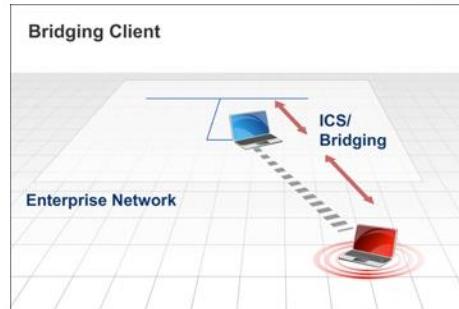
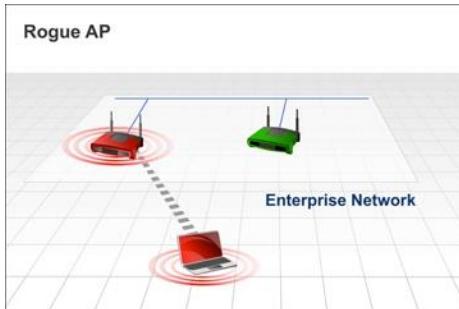
 **BJ's**  
WHOLESALE CLUB

**FOREVER 21**

**DSW**®



# Top Ten Wireless Threats





# Is your network security at risk from BYOD?

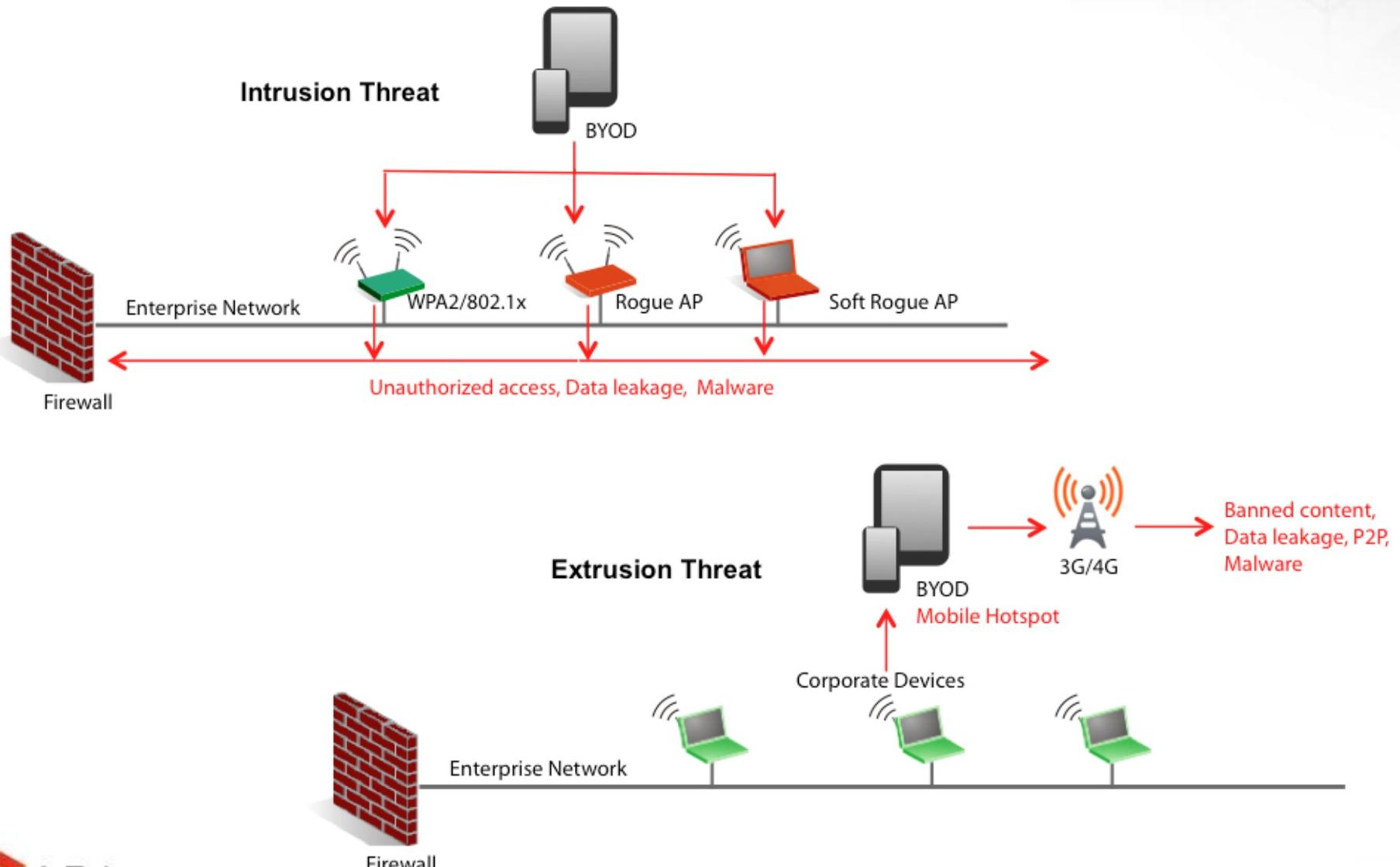


# Managing the “Unmanaged”

WPA2/802.1x cannot prevent unauthorized devices from accessing the enterprise network



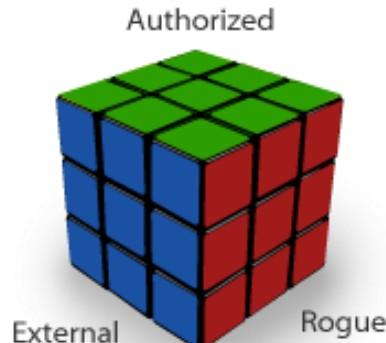
# Managing the “Unmanaged”





# Why AirTight WIPS?

# AirTight WIPS – The Only True WIPS



**Automatic  
Device Classification**



**Comprehensive  
Threat Coverage**



**Reliable  
Threat Prevention**



**Accurate  
Location Tracking**

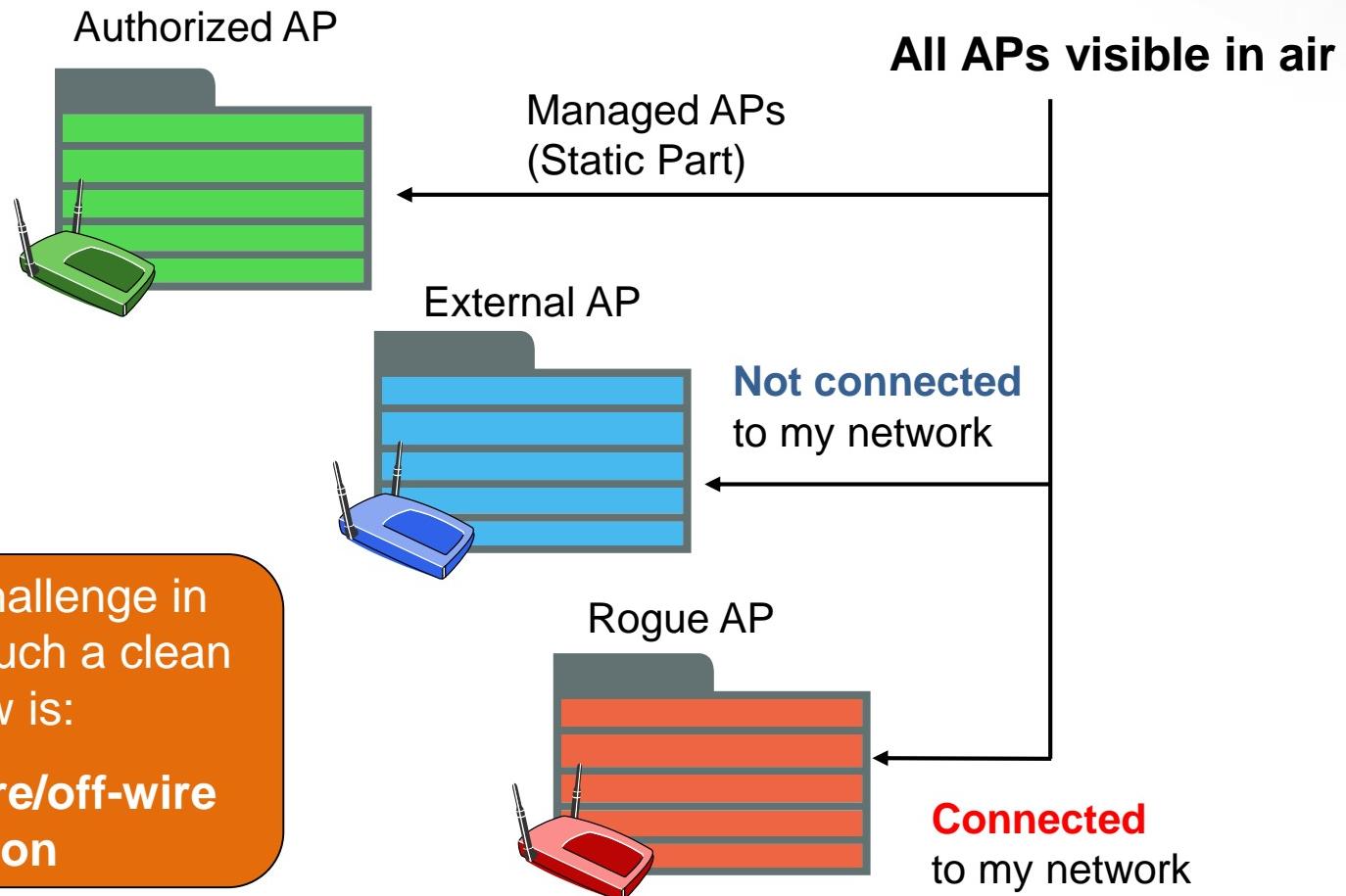


**BYOD  
Policy Enforcement**



**Automated  
Compliance Reporting**

# AirTight's Accurate Automatic Device Classification

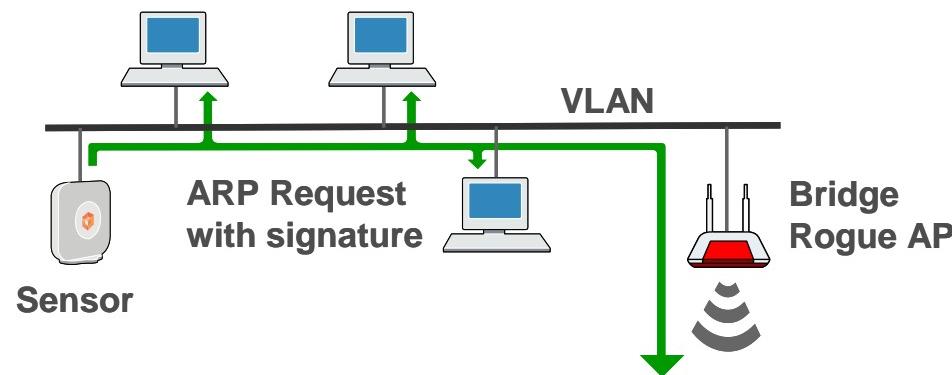


# AirTight's Patented Marker Packet™ Technique

Definitive “on-wire / off-wire” test

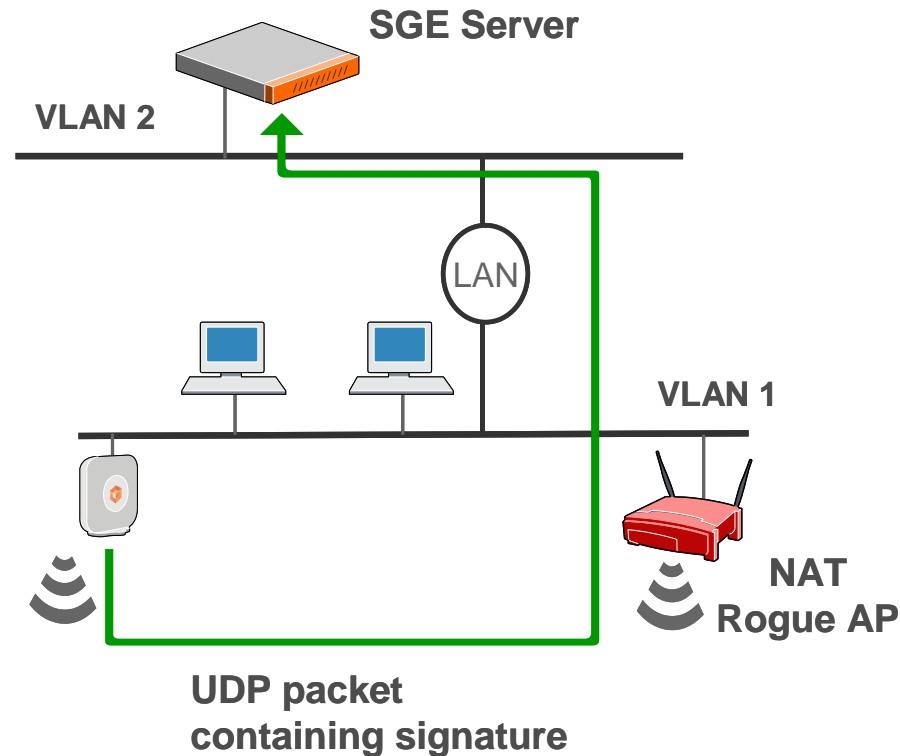
## ARP Request Marker Packet

Sensor sends ARP requests with signatures on the wire and detects if any get forwarded onto the wireless side



## UDP Reverse Marker Packet

Sensor sends UDP packets with signatures in the air and server detects if any get forwarded onto the wire



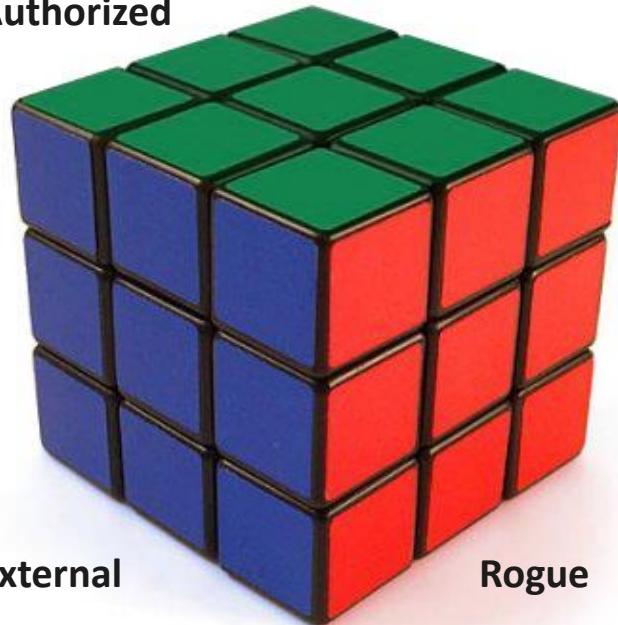
# Head-to-Head Comparison Of Rogue AP Detection

Criteria	Marker Packets	MAC Correlation
1. False negative on NAT APs	Never	Often
2. False positive on neighbor AP	Never	Often
3. Latency of detection	Low (few minutes)	High (tens of minutes)
4. Configuration, maintenance	Zero	High
5. Scalability	Infinite	Poor
6. Manual intervention for classification	None	Extensive

# Automatic Device Classification

## AirTight WIPS

Authorized



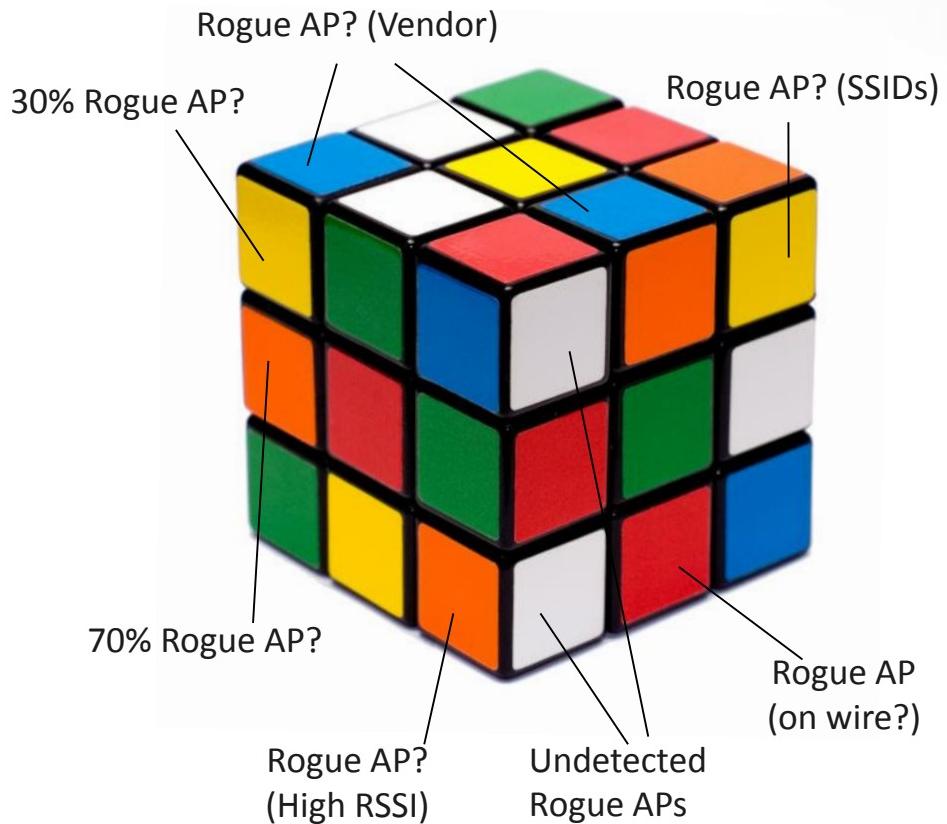
External

Rogue

Works “out of the box”

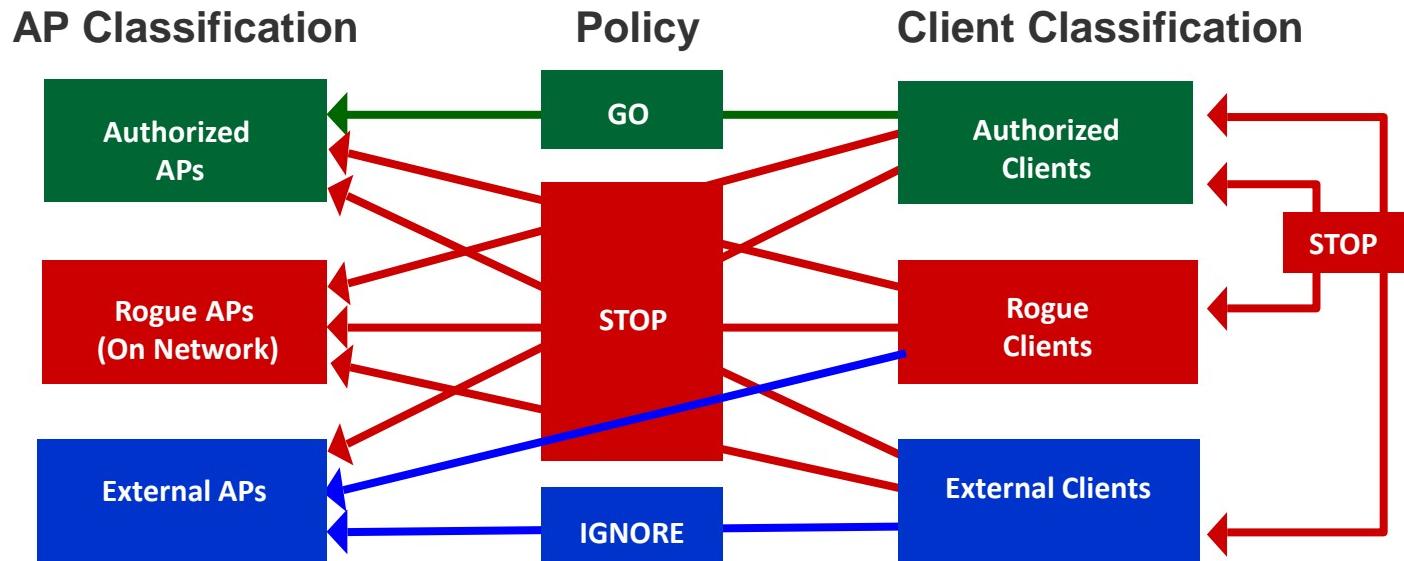
Rooted in active on-wire/off-wire detection

## Other WIDS solutions



Require users to configure complex rules  
and marred with false alarms

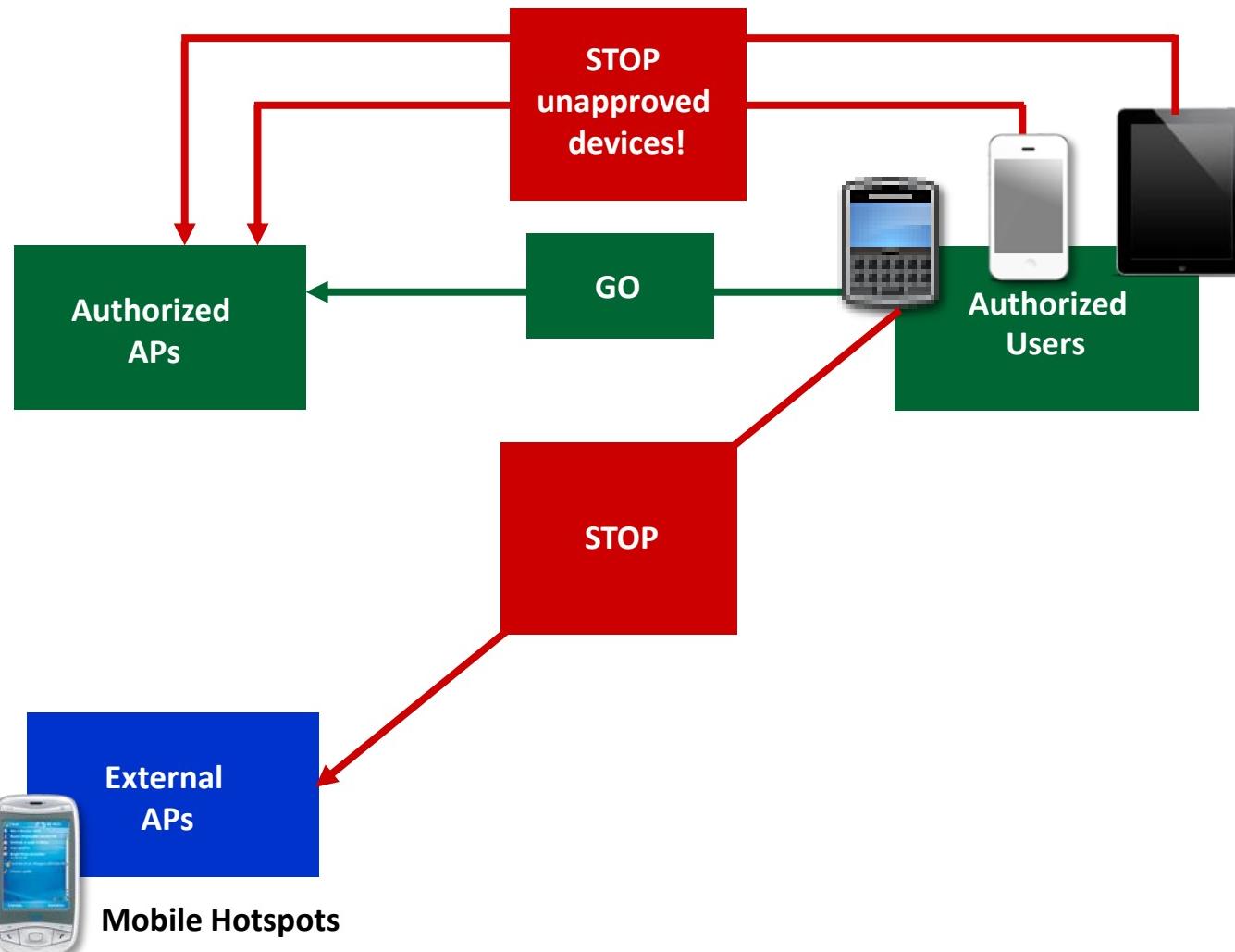
# AirTight's 24/7 WIPS Protection



**AUTOMATICALLY DETECTS AND BLOCKS RED PATHS!**

With this in place, your network is protected from all types of wireless threats, vulnerabilities and attack tools!

# Extending the WIPS for BYOD Policy Enforcement



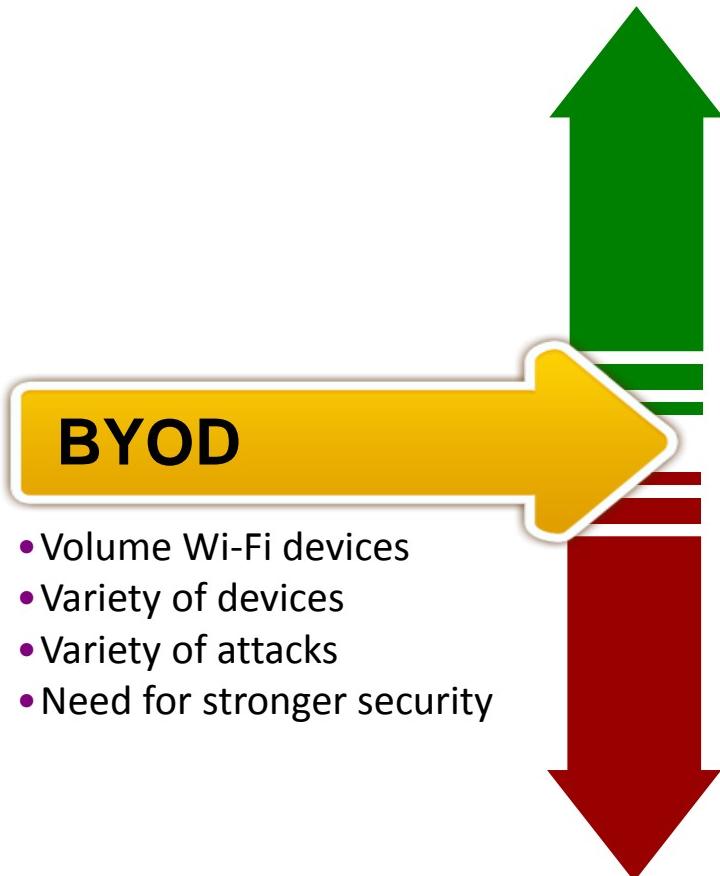
# Automatic Device Fingerprinting and Classification

- MDM and NAC are unable to provide the first line of defense
- WIPS complements these solutions to fully automate secure BYOD



Android	30:39:26:4B:86:C1	30:39:26:4B:86:C1
Blackberry	BLACKBERRY-9FCB	30:69:4B:9C:FE:F7
Blackberry	BLACKBERRY-3300	40:6A:AB:E3:BA:C3
iPad	Var	74:E1:B6:BE:4B:AD
iPad	Sushmas-iPad.io	FC:25:3F:AA:2E:AC
iPad	ATN	44:2A:60:9B:A1:C8
iPhone	Louiss-iPhone.l	58:1F:AA:61:A7:F7
iPhone	iPhone	00:1C:B3:65:73:94
iPhone	LAP119-PC	0C:77:1A:3B:42:0D
iPod-Touch	NP-	00:26:BB:BA:C7:A7
Windows-Mobile	Karan-HTC_90:11:1D	F8:DB:7F:90:11:1D
Window Mobile	Nokia_29	5C:E9:07:29:

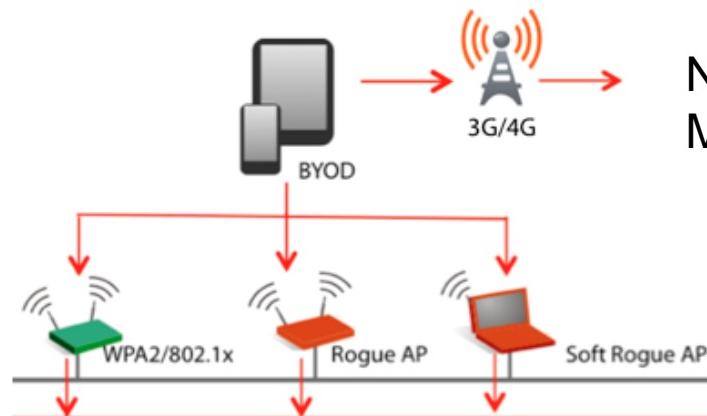
# BYOD Amplifies AirTight WIPS Advantages



## Limitations of “checkmark WIDS”

- Unreliable signature approach
- Manual inspection not practical
- Unreliable prevention
- Lack of automation
- Complex, difficult to manage

# MDM ≠ Network Security



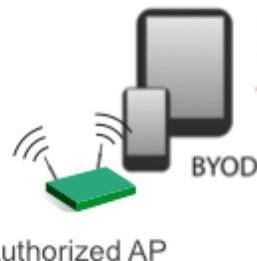
No visibility into Rogue APs, Soft Rogues, Mobile Wi-Fi Hotspots

Scope limited to “managed” devices that run MDM agent



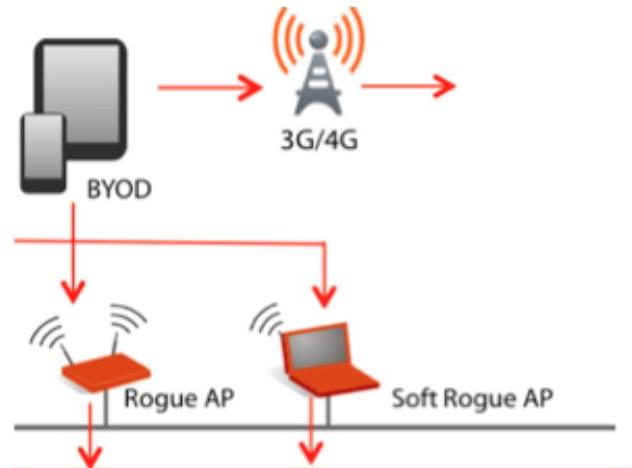
What is the incentive to install MDM agents on personal devices?

# NAC ≠ Wireless Security



Scope limited to BYOD on “managed” WLAN

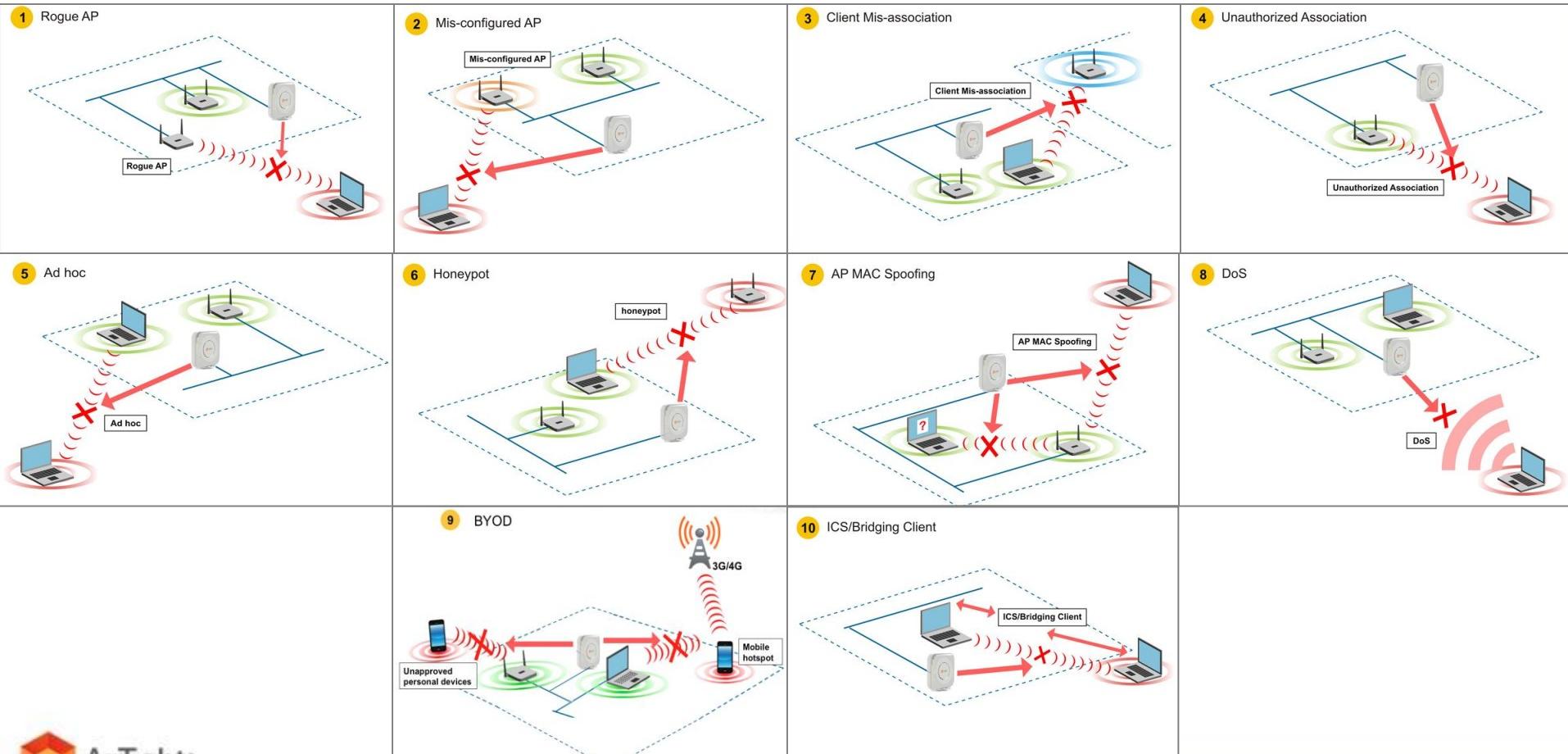
Cannot block Rogue APs, Soft Rogues,  
Mobile Wi-Fi Hotspots



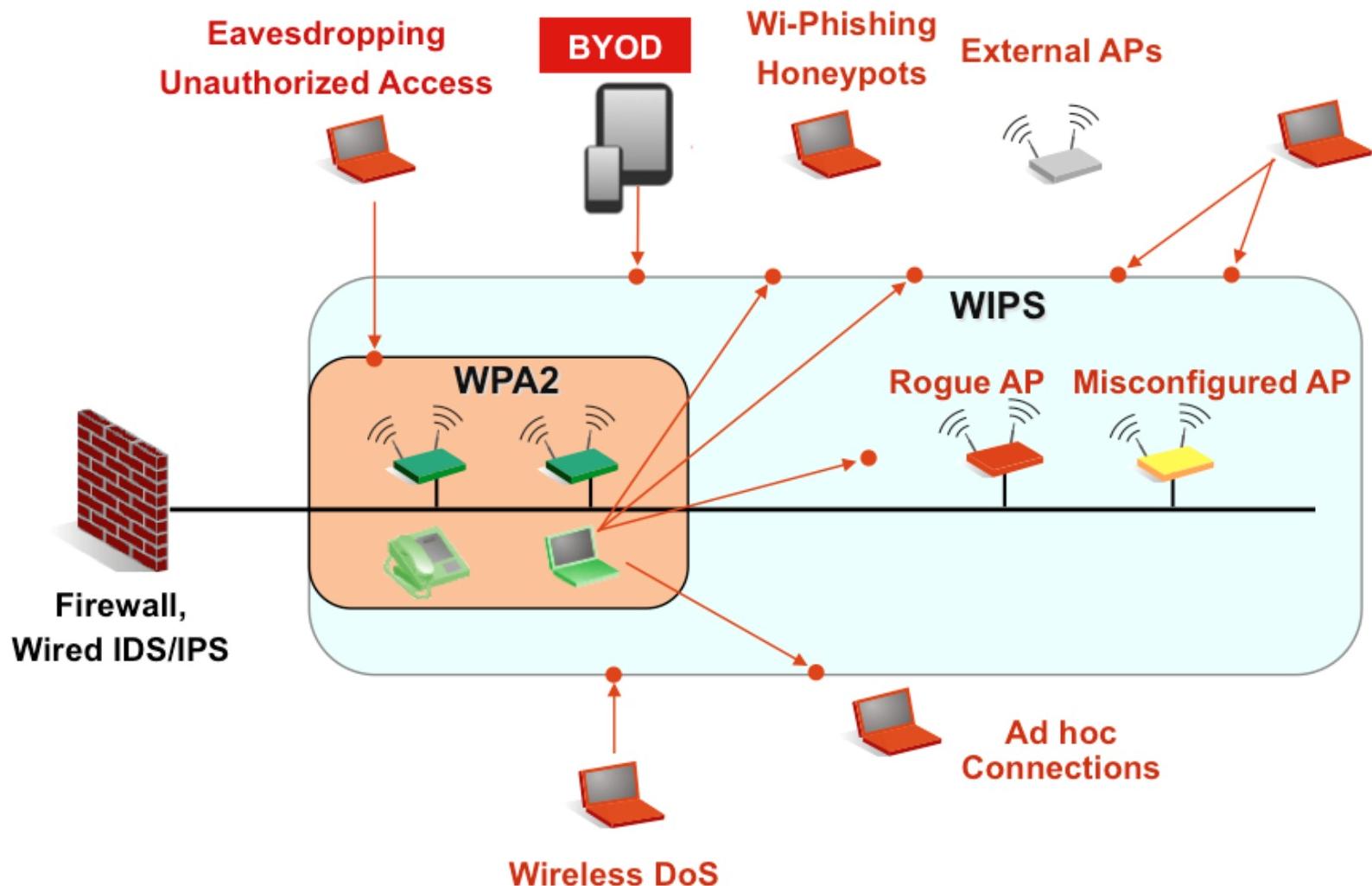
Suffers from “blind spots” – unauthorized Wi-Fi devices connecting via authorized devices

# Comprehensive Protection with AirTight WIPS

- Surgical threat prevention without interfering with legitimate communication (yours or your neighbor's)
- Simultaneous prevention of multiple threats across multiple channels

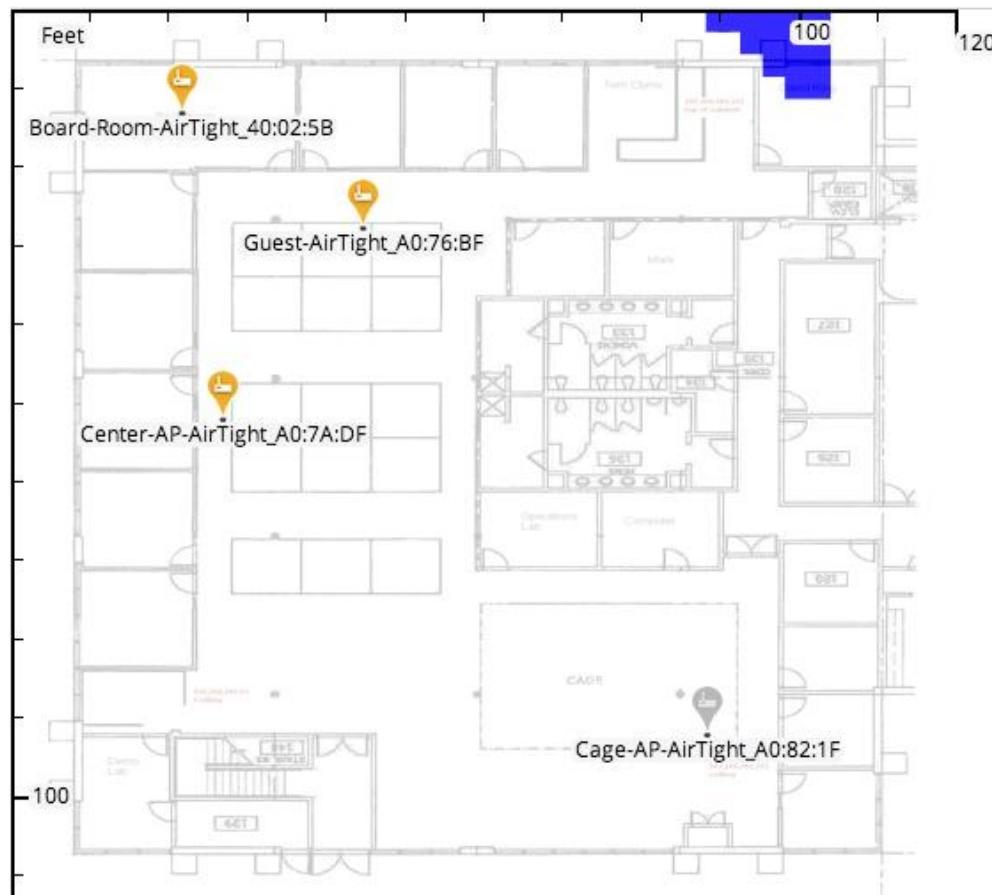


# Comprehensive Protection with AirTight WIPS



# AirTight's Accurate Location Tracking

Real Time and Historic

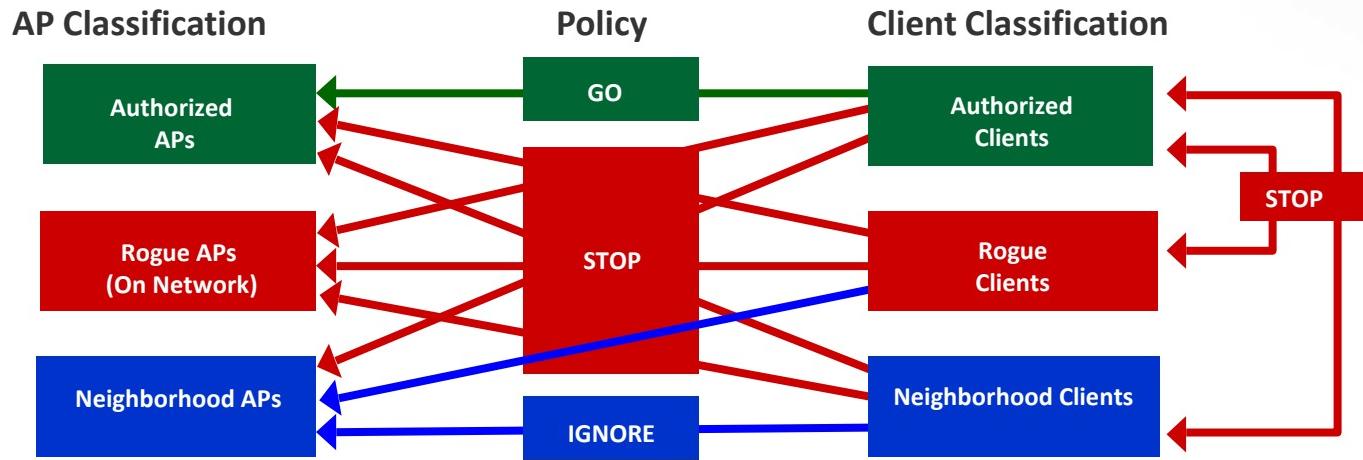


- No need for RF site survey
- No search squads to locate Wi-Fi devices
- Definitive location tracking within 10-15 ft.



## Compare that to Other WIDS Solutions

# AirTight Takes a Fundamentally Different Approach



With this in place, your network is protected from all types of threats, vulnerabilities and attack tools!

## Competition

- Require user to configure and maintain classification rules
- Large number of events using signature matching and anomaly thresholds
- Prone to false alarms, require continuous manual intervention
- Unreliable for automated threat prevention
- Classic problems of signature approach: Incomplete and changing signatures
- Minimal “zero-day attack” protection

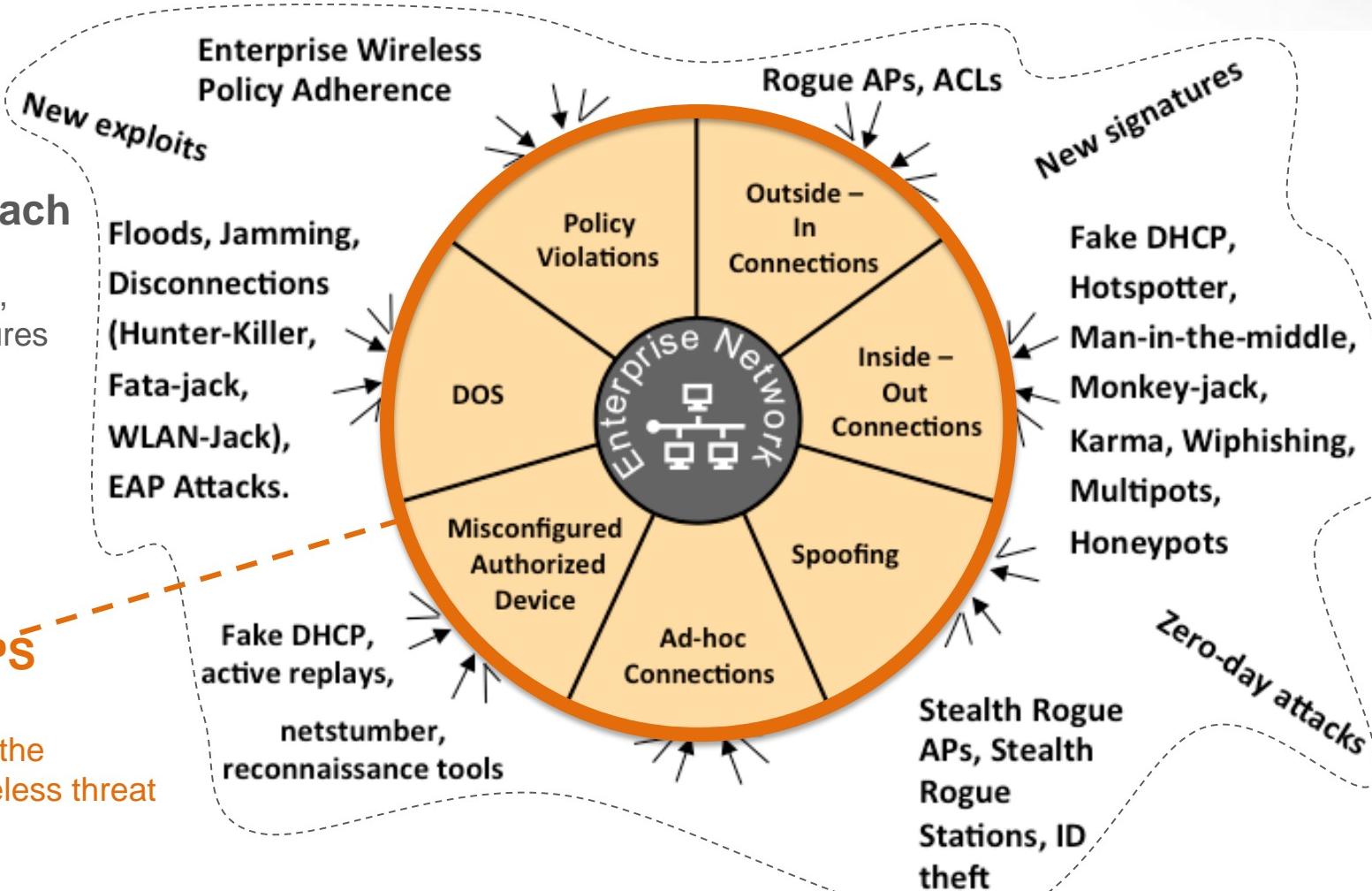
# AirTight Takes a Fundamentally Different Approach

## Prevalent WIDS Approach

Cat and mouse chase of exploits, tools and signatures

## AirTight WIPS Approach

Protects against the fundamental wireless threat building blocks



# AirMagnet (Fluke Networks)

Device Classification Settings

Rule Name :

Set ACL Type To :

Set ACL Group To :

- 
- 
- 
- 

Apply To Device Type :

[Criteria To Use](#)

The Device will be classified when one of the criteria is met

By Selected Vendor List

By SSIDs(Entries are separated by comma)

By Minimum Signal Strength (from -100 to -10 dbm)

- IDS - Denial of Service Attack
- IDS - Security Penetration
- Rogue AP and Station
- Rogue AP**
  - Rogue AP by MAC address (ACL)
  - Rogue AP by IEEE ID (OUI)
  - Rogue AP by SSID
  - Rogue AP by wireless media type
  - Rogue AP detected inside
  - Rogue AP by channel
  - Rogue AP traced on Enterprise wired
- Rogue Station**
  - Rogue station by MAC address (ACL)
  - Rogue station by IEEE ID (OUI)
  - Rogue station by SSID
  - Rogue station by wireless media typ
  - Rogue station by channel
- User Authentication & Encryption

# Cisco Adaptive WIPS

The screenshot shows the Cisco Adaptive WIPS interface. On the left, a navigation tree includes sections like Security, AAA, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies (selected), and Rogue Policies. The main pane displays a 'Rogue Rule > Edit' form with the following fields:

- Rule Name: Test\_Rule
- Type: Malicious (selected)
- Match Operation: Match Any (selected)
- Enable Rule:

Below these are 'Conditions' and an 'Add Condition' button. A dropdown menu lists 'SSID' as the selected condition. To the right, a sidebar lists various policies and features:

- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Rogue Policies
- General
- Rogue Rules
- Friendly Rogue
- Standard Signatures
- Custom Signatures
- Signature Events
- Summary
- Client Exclusion Policies

A red warning message on the right side of the interface states: "Many WLAN vendors offering ‘so-called WIPS’ recommend their customers to NOT turn on automatic threat prevention!"

**Auto Contain**

Action	Status
Rogue on Wire	<input checked="" type="checkbox"/> Enabled
Using our SSID	<input type="checkbox"/> Enabled
Valid client on Rogue AP	<input type="checkbox"/> Enabled
AdHoc Rogue AP	<input type="checkbox"/> Enabled

**The page at <http://172.21.2.180> says:**

Warning! Using this feature may have legal consequences.  
Do you want to continue?

OK Cancel

# Cisco Adaptive WIPS



Arbitrary Threshold and Packet Count Based  
Signatures to Hide False Alarms

DoS Detection Type	Alarm Threshold (PPM)	Alarm Interval (Sec)	Enabled
Probe Request	12000	60	<input checked="" type="checkbox"/>
Probe Response	24000	60	<input checked="" type="checkbox"/>
(Re)Association Request	6000	60	<input checked="" type="checkbox"/>
Association Response	2400	60	<input checked="" type="checkbox"/>
Disassociation	1200	60	<input checked="" type="checkbox"/>
Authentication	6000	60	<input checked="" type="checkbox"/>
De-authentication	1200	60	<input checked="" type="checkbox"/>
EAP over LAN (EAPOL)	6000	60	<input checked="" type="checkbox"/>

# Aruba Networks – Petty Signatures to Hide False Alarms

## ARUBA NETWORKS WIPS PRODUCT GUIDE

	Good AirWave RAPIDS	Good ArubaOS (Base OS)	Better ArubaOS (WIP License)	Best ? RFprotect Distributed
Possible IP Worm traffic				Yes
Service VAN nearby				Yes
Spoofed MAC address			Yes <sup>1</sup>	Yes



# Motorola AirDefense

Administrator has to define complex signature-based rules for wireless threat detection

<b><i>MAC</i></b>	<b><i>Signal Strength</i></b>	<b><i>Connectivity</i></b>
<b><i>IP Address</i></b>	<b><i>Protocol</i></b>	<b><i>Association</i></b>
<b><i>Vendor</i></b>	<b><i>Authorization</i></b>	<b><i>Key Generation</i></b>
<b><i>Channel</i></b>	<b><i>802.X Username</i></b>	<b><i>Specific EAP Type</i></b>
<b><i>SSID</i></b>	<b><i>Last Seen</i></b>	<b><i>Encryption</i></b>

Excerpt from the Motorola AirDefense User Guide

### 8.5.3.3 Scheduled

Because auto-classification places a minor burden on the system, AirDefense, Inc. recommends that you schedule auto-classification to occur only once or twice a day.

### 8.5.4.2 Action Rules

The Action Rules tab of the Auto Classification page lets you create a very specific set of rules for classifying devices. The more criteria you include, the more accurate the resultant classification will be, and the less likely it is that a device will be mis-classified.

# Location Tracking



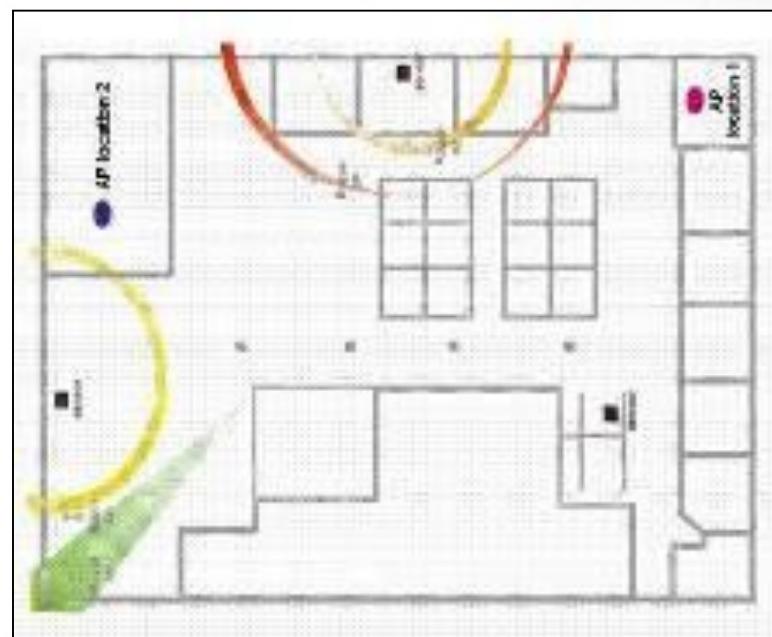
## Stochastic RF Triangulation with Fingerprinting

Self adjusting to signal variations due to TX power fluctuations, antenna orientation and RF obstructions

Does not require site survey for calibration

Displayed as location probability distribution map

## Competition



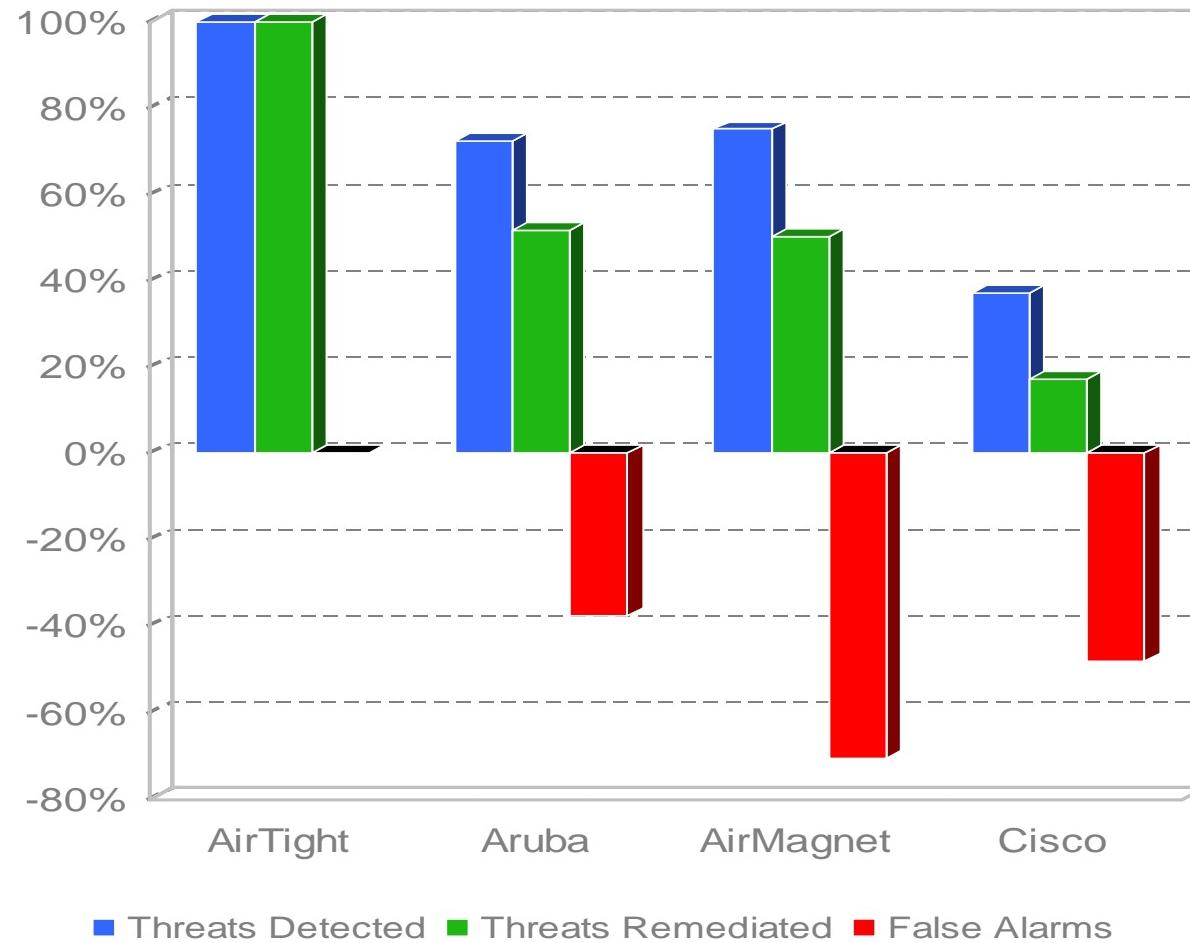
## Simple RF Triangulation

Received signal strength used to estimate distance to the device and location estimated as intersection of circles

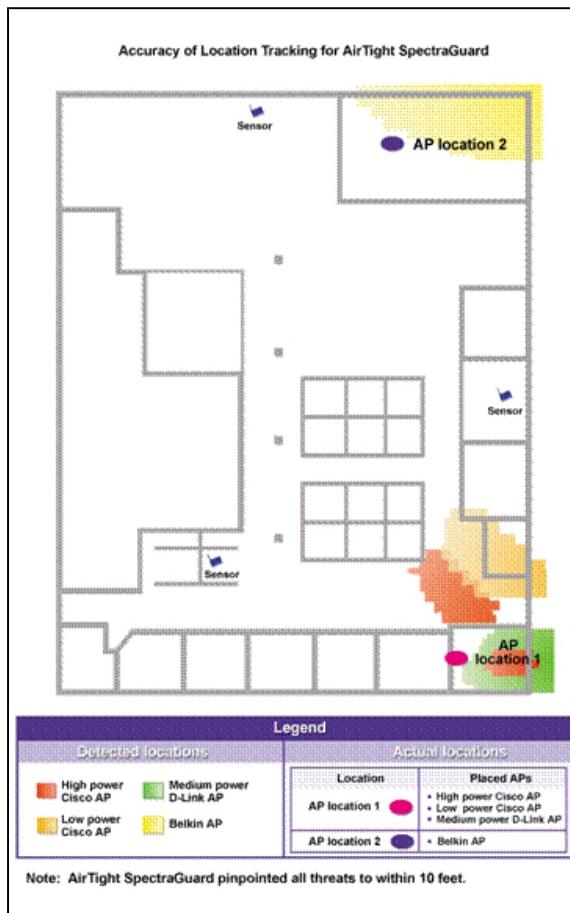
Sensitive to signal variations resulting in inaccurate location tracking

Requires site survey for calibration

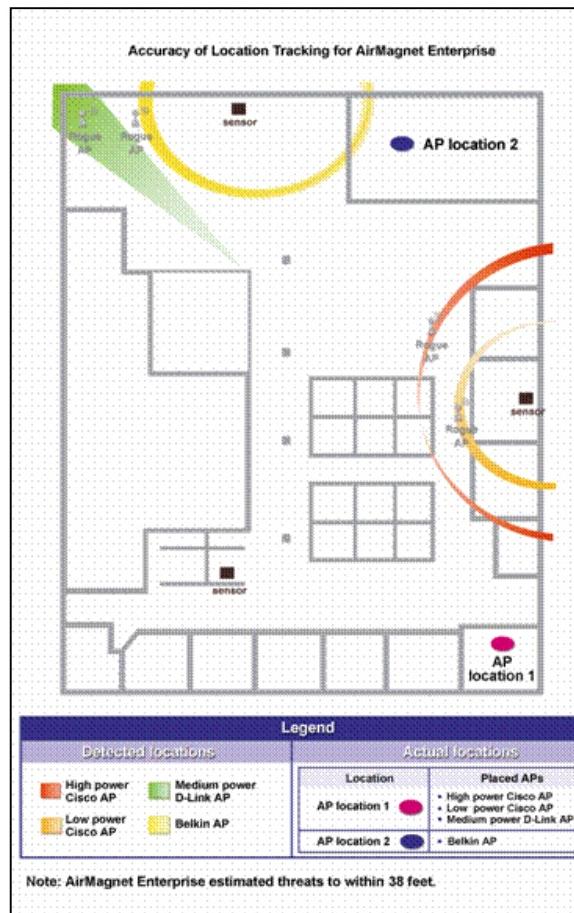
# Best Threat Detection and Prevention



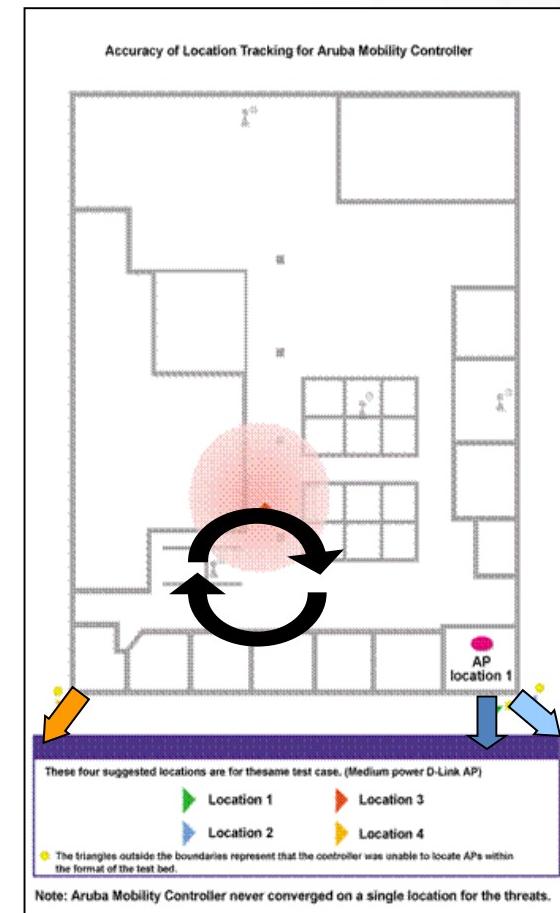
# Most Accurate Location Tracking



AirTight



AirMagnet



Aruba

\* Aruba repeatedly rotated through 4 locations for a single threat



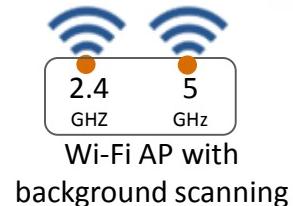
## Airtight WIPS Flavors

# WIPS Architectures



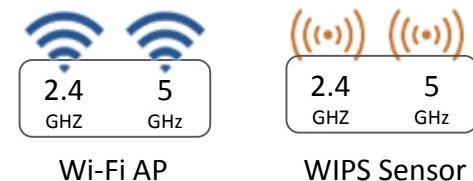
## ■ Integrated

- APs repurposed as sensors for background scanning
- Full threat detection and wire-side Rogue AP prevention
- Not recommended with time-sensitive apps, e.g., VoIP



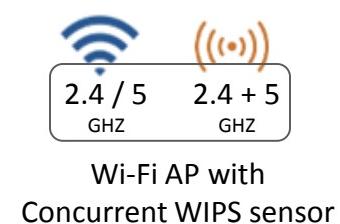
## ■ Overlay

- Dedicated sensors on top of existing WLAN
- 24/7 monitoring and protection



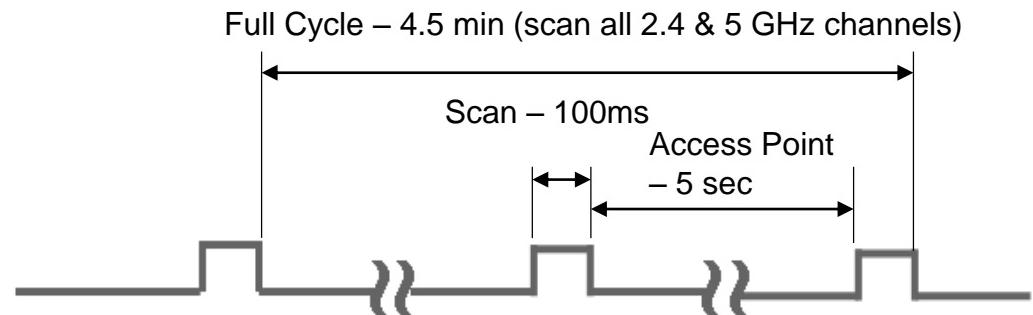
## ■ Combo

- APs repurposed as sensors
- 24/7 monitoring and protection
- Able to support all types of apps, including VoIP



# Integrated / Background WIPS

- Scans all 2.4 and 5 GHz band channels
- Monitors 8 VLANs for rogue APs using Marker Packet™
  - Patented packet injection time-synchronized with off-channel visits for reliable detection of Rogue APs
- Automated wire-side prevention of unlimited number of Rogue APs
- Works even with unmanaged switched
- Detects over-the-air policy violations, e.g., client mis-associations, ad-hoc connections



# AT-C60: Industry's Most Flexible Wi-Fi Platform



- Software-defined, band-unlocked radios
  - an industry first
- Concurrent Wi-Fi access and 24/7 WIPS
  - an industry first





# Airtight WIPS Platforms

# AirTight Deployment Choices



## Platforms



AT-C10



AT-C50



AT-C60



AT-C55

## Deployment



Public Cloud



Private Cloud



VMware



Appliance

## Pricing

- ✓ Zero Capex
- ✓ Bundled
- ✓ Capex

No feature based licensing!  
No user based licensing!

# AirTight Server Appliances



**SA-250**  
**Standard Appliance**



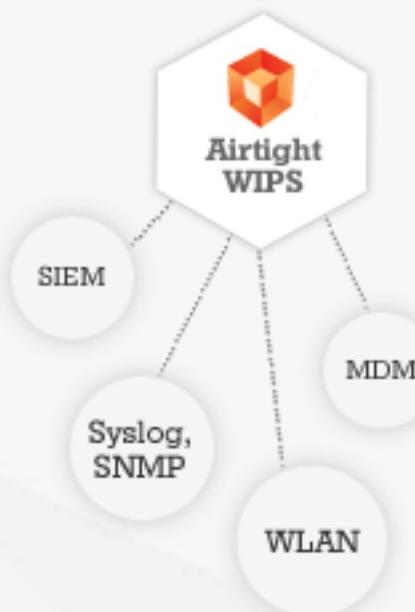
**SA-360**  
**Premium Appliance**

# AirTight Access Points

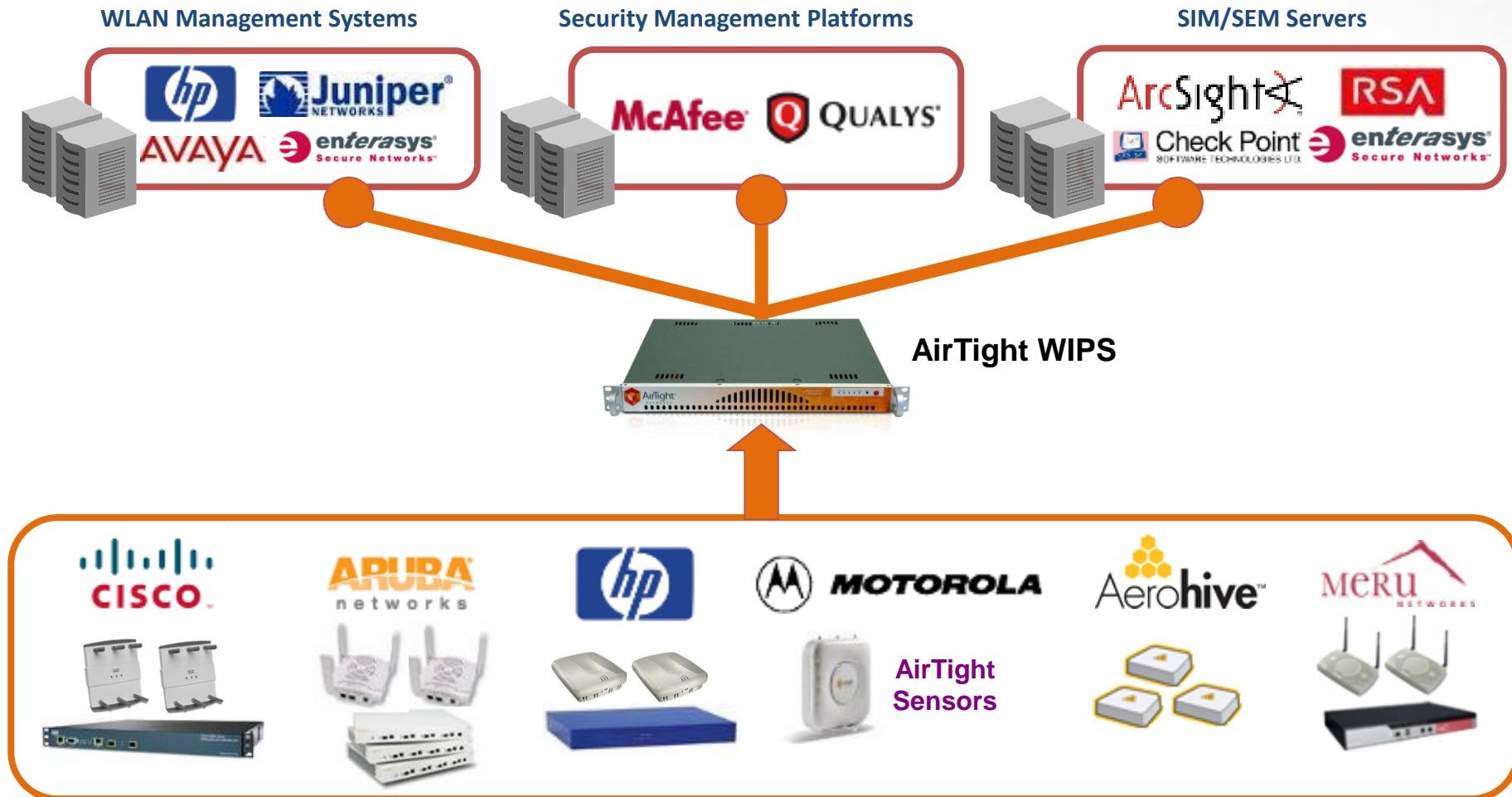


C-50	C-55 and C55-E	C-60	0-70 (outdoor)	C-75 and C-75-E
Single “n” radio	Dual “n” radio	Dual “n” radio	Dual “n” radio	Dual “ac/n” radio
2x3:3	2x2:2 2x2:2	3x3:3 2x2:2	3x3:3 3x3:3	3x3:3 3x3:3
300 Mbps	300 Mbps 300 Mbps	450 Mbps 300 Mbps	450 Mbps 450 Mbps	1.3 Gbps “ac” 450 Mbps “n”
<ul style="list-style-type: none"> <li>• Single AP</li> <li>• Single WIPS</li> </ul>	<ul style="list-style-type: none"> <li>• Dual AP</li> <li>• Dual WIPS</li> </ul>	<ul style="list-style-type: none"> <li>• Dual AP</li> <li>• Dual WIPS</li> <li>• 1 AP, 1 WIPS</li> </ul>	<ul style="list-style-type: none"> <li>• Dual AP</li> <li>• Dual WIPS</li> </ul>	<ul style="list-style-type: none"> <li>• Dual AP*</li> <li>• Dual WIPS (Phase 2)</li> </ul>
PoE	PoE	PoE	PoE+	PoE

# Integration with 3<sup>rd</sup> Party Systems

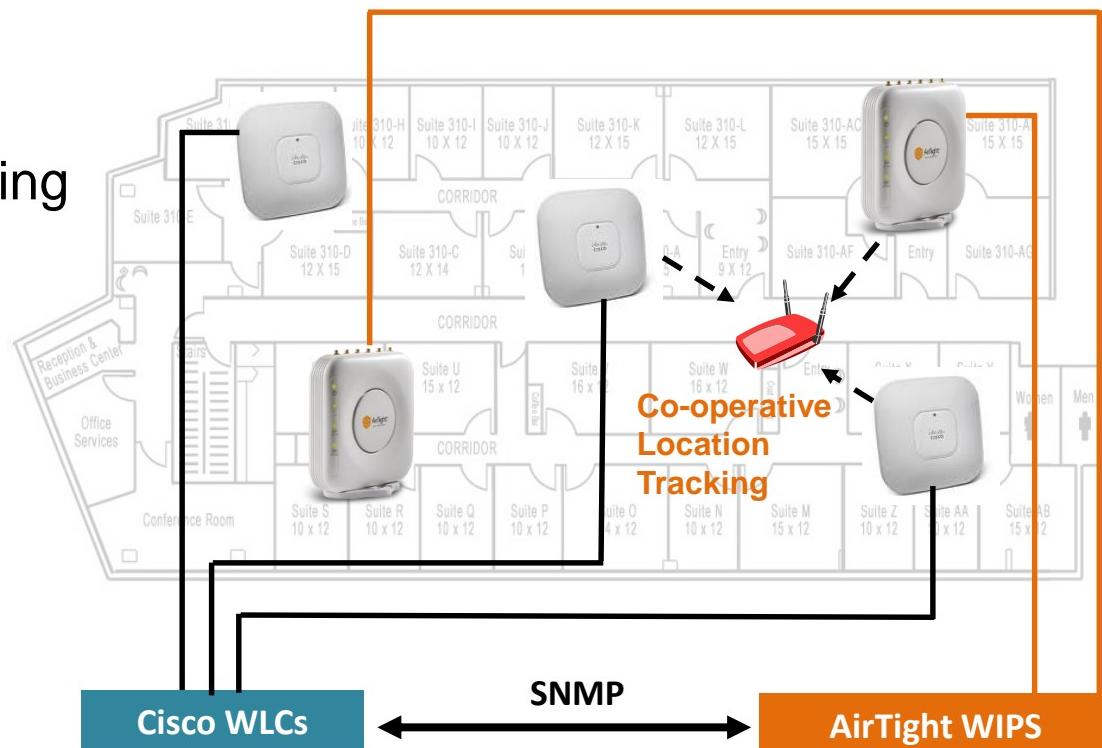


# Comprehensive Enterprise Integration



# Cisco WLC Integration

- Synchronize devices between Cisco WLCs and AirTight WIPS
  - Automatically identify and populate managed AP information in WIPS
- Use AirTight auto-classification, prevention, location tracking
- Reduces WIPS sensor density for location tracking
  - Use RSSI information from APs along with WIPS sensors



# Cisco WLC Integration

**SpectraGuard Enterprise** System Superuser (Superuser)

**Cisco WLC**

**Cisco WLC Integration**

Integration with CISCO WLC allows the server to automatically classify devices managed by designated Cisco Wireless LAN Controllers and accept RSSI of devices visible to LWAPP APs managed by the WLC to enhance location tracking capabilities.

**WLC Integration Status**

If WLC Integration is enabled, the system shall obtain data from the configured WLCs below.

WLC Integration Enabled

Current Status Running

Imported AP Level 69% [What is this?](#)

**Wireless LAN Controllers** [Total: 3]

IP Address:Port	Enabled?	Status	Last Synchronization
192.168.55.180:161	Enabled	Active	Jun 13, 2009 1:26 PM
172.21.2.180:161	Enabled	Active	Jun 13, 2009 1:26 PM
192.168.22.31:161	Disabled		

**Test WLC Settings Result**

WLC IP Address	Test	WLC Version
192.168.55.180	PASS	4.2.176.0
172.21.2.180	PASS	5.2.178.0
192.168.22.31	FAIL	--

If **PASS**, WLC Controller reachable via SNMP.  
WLC can be added successfully.

If **FAIL**, WLC Controller not reachable via SNMP.  
Please check IP, community string or port number  
settings for that WLC.

**Meter to show the load from existing WLC integrations**

**Test function shows status of the configuration of each WLC controller**

**Added Support for WLC v5.2 and v6.0**

# Aruba Mobility Controller Integration

SpectraGuard® Enterprise System Superuser (Superuser)

Dashboard Events Devices Locations Reports Forensics Administration

Global Local

Global Policies Event Settings Device Settings User Management Location Settings System Settings WLAN Integration Aruba Cisco WLC Cisco WLSE HiveManager HP MSM Controller Meru ESM Integration SpectraGuard SAFE Group Management Settings Manage Clients

## Aruba Integration

System can fetch wireless device inventory and RSSI information from Aruba Mobility Controllers for ease of management and improved location tracking.

### Aruba Integration Status

If Aruba Mobility Controller Integration is enabled, the system shall obtain data from the controller(s) configured below.

Aruba Integration Enabled

Current Status  Stopped

Imported APs 0% of maximum allowed. [What is this?](#)

### Aruba Mobility Controllers

Manage the list of Aruba Mobility Controllers and their settings below. [Total:0]

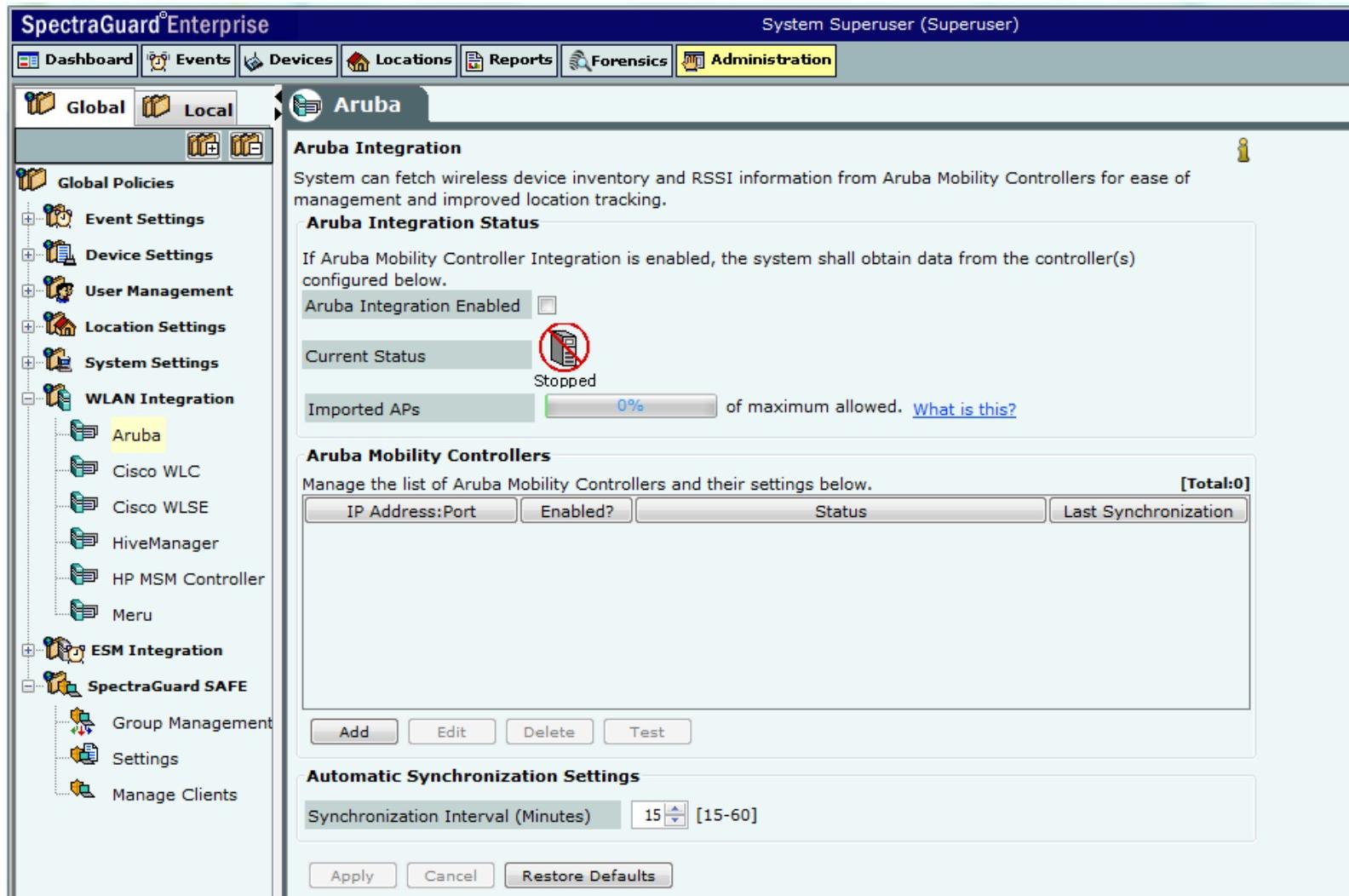
IP Address:Port	Enabled?	Status	Last Synchronization

Add Edit Delete Test

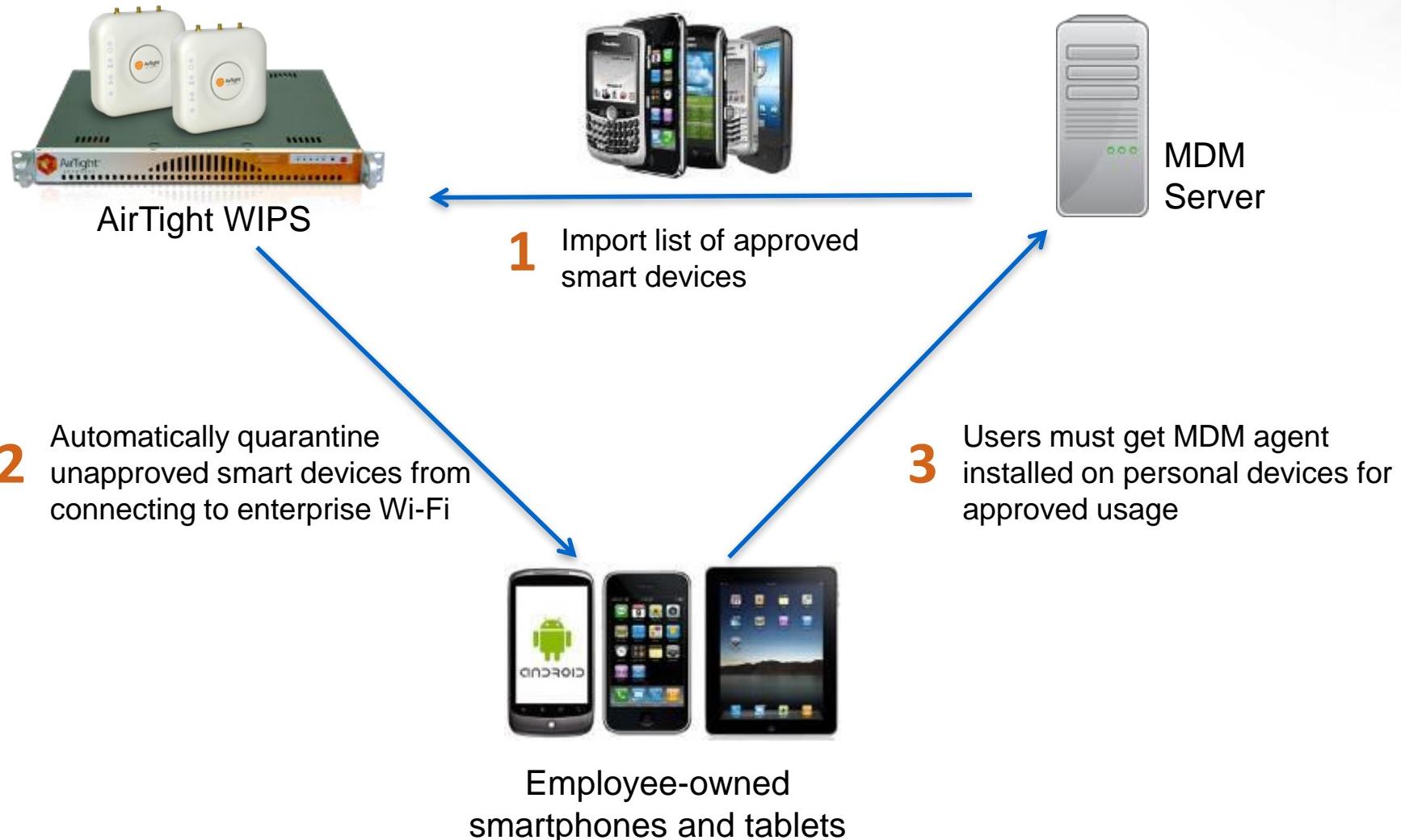
### Automatic Synchronization Settings

Synchronization Interval (Minutes) 15 [15-60]

Apply Cancel Restore Defaults



# Secure BYOD Onboarding via MDM Integration





## Airtight WIPS Screenshots

# Automatic AP Classification

AirTight Devices											
APs											
Clients											
<input type="checkbox"/> All	<input checked="" type="checkbox"/> Authorized	<input checked="" type="checkbox"/> Rogue	<input checked="" type="checkbox"/> External	<input type="checkbox"/> Uncategorized							
	RSSI	Name	MAC Address	Channel	Protocol	No. of ...	SSID	Security	Location	Network	Up/Down Since
<input type="checkbox"/>		AirTight_A0:82:00	MULTIPLE	MULTI...	a/b/g [...	0	MULTIPLE	802.11i	*CA - Mountain View/...	--	Apr 14, 2013 03:40:...
<input type="checkbox"/>		AirTight_A0:82:00	00:11:74:A0:8...	36	a [802....	0	anw	802.11i	*CA - Mountain View/...	--	Apr 14, 2013 03:40:...
<input type="checkbox"/>		AirTight_A0:82:00	00:11:74:A0:8...	1	b/g [80...	0	@NAT	802.11i	*CA - Mountain View/...	--	Apr 14, 2013 03:40:...
<input type="checkbox"/>		AirTight_A0:82:00	00:11:74:A0:8...	1	b/g [80...	0	anw	802.11i	*CA - Mountain View/...	--	Apr 14, 2013 03:40:...
<input type="checkbox"/>		AirTight_A0:82:00	00:11:74:A0:8...	36	a [802....	0	@VOIP	802.11i	*CA - Mountain View/...	--	Apr 14, 2013 03:40:...
<input type="checkbox"/>		Cisco_3F:68:BD	44:E4:D9:3F:6...	64	a [802....	0	edgenet	802.11i	CA - Mountain View/A...	--	Apr 14, 2013 03:40:...
<input type="checkbox"/>		Cisco_FF:41:6D	B4:14:89:FF:4...	56	a [802....	0	edgenet	802.11i	CA - Mountain View/A...	--	Apr 14, 2013 03:40:...
<input type="checkbox"/>		Ruckus_66:7A:B9	00:24:82:66:7...	2	b/g	0	SAn0kit-ss3ccA-Eth...	802.11i	AirTight Pune/Gamma	--	Apr 14, 2013 08:26:...
<input type="checkbox"/>		Cisco_09:37:10	00:23:EB:09:3...	4	b/g	0	Deutsche Telekom	802.11i	CA - Mountain View/A...	--	Apr 14, 2013 03:40:...
<input type="checkbox"/>		D-Link_7F:7A:62	14:D6:4D:7...	6	b/g [80...	0	dlink-bgn	802.11i, ...	AirTight Pune/Beta	--	Apr 12, 2013 03:02:1...

# Automatic Client Classification

AirTight Devices | APs | Clients

All  Authorized  Guest  Rogue  External  Uncategorized

	RSSI	Smart Device Type	Name	MAC Address	Associated AP	SSID
DLHP	--	--	10:68:3F:3F:A7:3B	10:68:3F:3F:A7:3B	--	--
LG_96:9A:DC	--	--	18:3D:A2:A7:DF:00	AirTight_A0:7A:C0	anw	
AGGIELD610	--	--	E8:92:A4:96:9A:DC	--	--	
Tropos_04:84:5E	--	--	EC:1A:59:39:11:C8	AirTight_A0:22:80	AA_BGN_3	
Terris-iPod	iPod-Touch	--	00:0D:97:04:84:5E	--	--	
Apple_41:BC:9C	--	--	90:27:E4:82:0B:05	AirTight_A0:76:A0	airtightguest	
Apple_6F:82:43	--	--	18:20:32:41:BC:9C	--	--	
Apple_76:17:6B	--	--	0C:74:C2:6F:82:43	Tropos_04:83:AD	GoogleWiFi	
Apple_DD:6B:91	--	--	00:26:4A:76:17:6B	Tropos_04:83:AD	GoogleWiFi	
LG_99:39:30	--	--	F8:1E:DF:DD:6B:91	--	--	
NOONU	--	--	E8:92:A4:99:39:30	Tropos_04:83:AD	GoogleWiFi	
	--	--	8C:70:5A:55:7D:F8	Cisco_83:45:7F	CiscoBR	

Select All | 0 selected | More | Filter: OFF | 2 | 26 - 50 of 4916

Client Properties

Currently Active	Yes
Client Name	DLHP
User Name	host/DLHP.airtightnetworks.net
Classification	Authorized
Device Tag	
MAC Address	18:3D:A2:A7:DF:00
Location	CA - Mountain View/AirTight Networks
Up Since	Apr 26, 2013 9:26:37 AM

Recently Associated to APs/ Ad hoc Networks [Total: 1]

AP Name/Ad hoc ID	SSID	Last Detected At
AirTight_A0:7A:C0	anw	Present

# Wireless Security Alerts



AirTight Management Console

Dashboard Devices Events Locations Reports Configuration

Kaustubh Phanse Apr 14 2013, 09:06:15 PM

U3 Demo Server > AirTight Networks >

Quick Search

Search Locations

U3 Demo Server

AirTight Networks

India USA

Security System Performance

ID	Details	Category	Location	Start Time
64278	Rogue AP [Senao_E5:63:52] is active.	Rogue AP	AirTight Pune/Beta	Apr 12, 2013 12:43:56 AM
64277	[Rogue] Client [RLDP] running Soft Mobile Hotspot AP ... Misbehaving Clients	Misbehaving Clients	AirTight Pune/Beta	Apr 12, 2013 12:43:56 AM
64276	Rogue AP [Cisco_88:73:F2] is active.	Rogue AP	AirTight Pune/Beta	Apr 12, 2013 12:43:56 AM
64275	[Rogue] Client [RLDP] running Soft Mobile Hotspot AP ... Misbehaving Clients	Misbehaving Clients	AirTight Pune/Beta	Apr 12, 2013 12:43:56 AM
64274	Rogue AP [Cisco_88:73:F1] is active.	Rogue AP	AirTight Pune/Beta	Apr 12, 2013 12:43:56 AM
64273	Rogue AP [Senao_E5:63:50] is active.	Rogue AP	AirTight Pune/Beta	Apr 12, 2013 12:43:56 AM
64272	[Rogue] Client [RLDP] running Soft Mobile Hotspot AP ... Misbehaving Clients	Misbehaving Clients	AirTight Pune/Beta	Apr 12, 2013 12:43:56 AM
64271	Rogue AP [Cisco_88:73:F0] is active.	Rogue AP	AirTight Pune/Beta	Apr 12, 2013 12:43:56 AM
64270	Rogue AP [D-Link_7F:7A:62] is active.	Rogue AP	AirTight Pune/Beta	Apr 12, 2013 12:43:56 AM

Select All 0 selected

More Filter: OFF 51 1251 - 1275 of 25463

Sub-events	Time	Devices in Selected Sub-event		
Event Started.	Apr 12, 13 12:43:56 AM	D-Link_7F:7A:62	14:D6:4D:7F:7A:62	<a href="#">Current Location</a> <a href="#">Event Time Location</a>
<b>Rogue AP [D-Link_7F:7A:62] has become active.</b>	<b>Apr 12, 13 12:43:56 AM</b>			
AP [D-Link_7F:7A:62] has become inactive.	Apr 12, 13 03:02:12 AM			
Event Expired.	Apr 12, 13 03:02:12 AM			

Other Devices in Event

+ A X

# Rogue AP Location Tracking



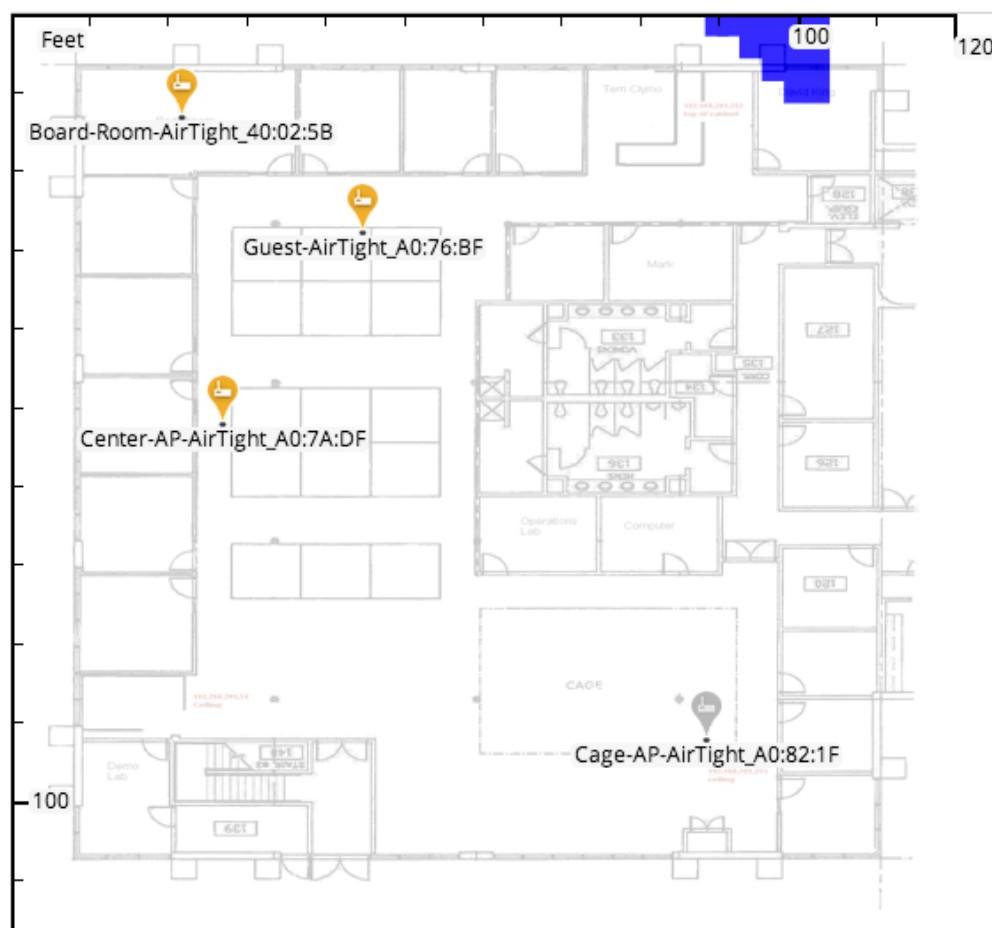
Tracking location of D-Link\_7F:7A:62 at Apr 12, 2013 12:43:56 AM

Floor plan:

AirTight Pune\Beta

[Switch to proximity view](#)

Opacity



Controls Panel

Resolution

Location Probability



# Dashboard



AirTight Management Console    Dashboard    Devices    Events    Locations    Reports    Configuration    Kaustubh Phanse    Apr 23 2013, 11:12:07 PM   

U3 Demo Server > AirTight Networks >

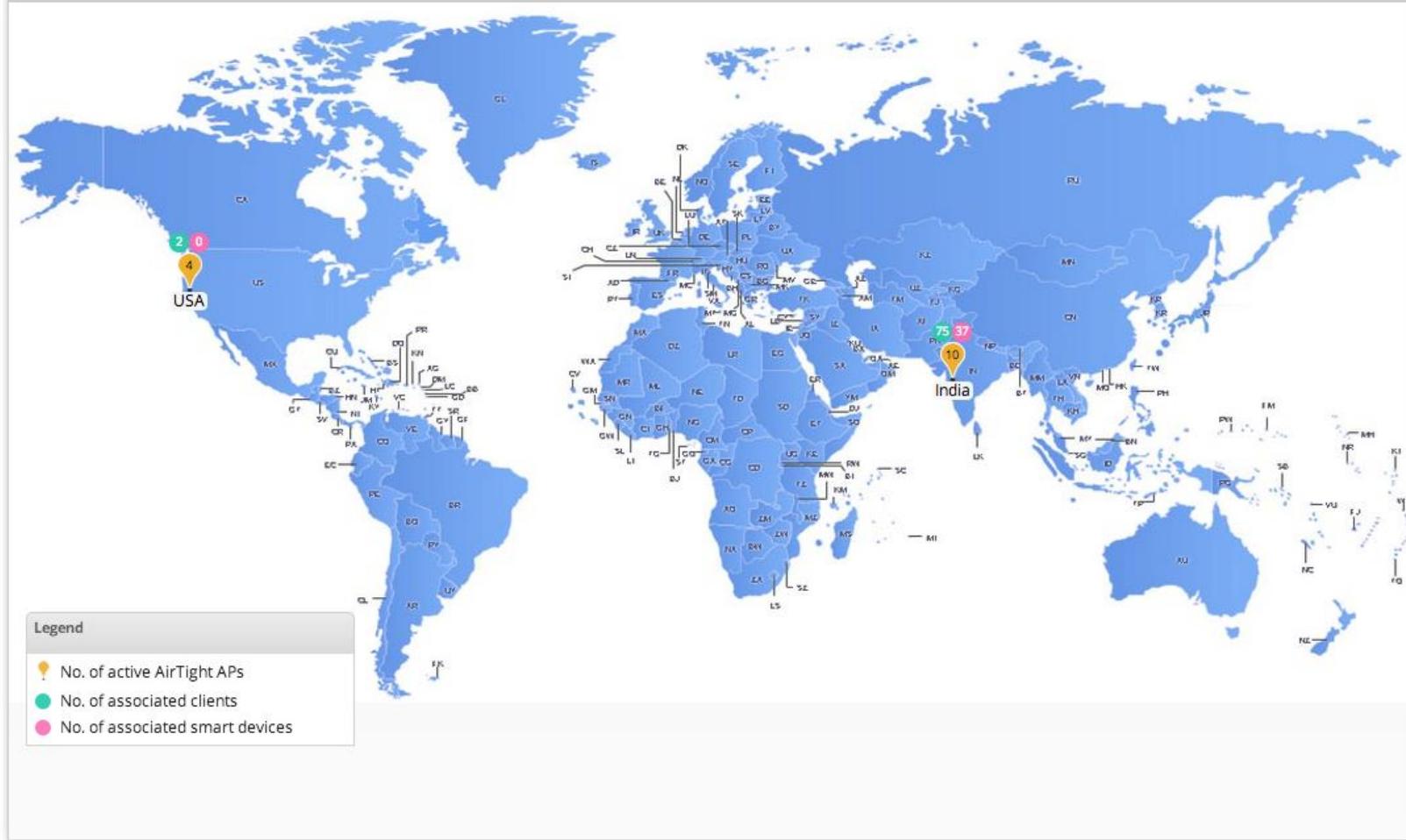
Search Locations

Dashboard 2

1 2 3 4

Location Map

i



# WIPS Dashboard

AirTight Management Console    Dashboard    Devices    Events    Locations    Reports    Configuration    Kaustubh Phanse    Apr 26 2013, 09:23:56 AM   

U3 Demo Server > AirTight Networks >

Wireless Security Dashboard

Security Status: Vulnerable

AirTight Devices: Active

ID	Details	...	...
76807	Rogue Client [LG_99:39:30] is active.	...	...
76806	Rogue Client [RIM_A4:CE:A4] is active.	A...	...
76805	Rogue Client [bads-iPhone] is active.	A...	...
76804	Rogue Client [Samsung_A9:0E:8B] is ...	A...	...
76803	Rogue Client [Apple_E3:86:1C] is acti...	A...	...
76801	Rogue Client [Samsung_CB:CF:981 is ...	A...	...

Latest Security Events: 4 hours

AP Classification: Active

Top Security Event Categories: 4 hours

Smart Devices Distribution: All SSIDs

Client Classification: Active

Top Locations by Events: 4 hours

AP Security Distribution: All SSIDs

# Secure Enterprise WLAN Checklist



## Can your enterprise WLAN solution:

- ✓ Accurately detect all types of Rogue APs without you having to define any signatures?
- ✓ Not flood you with false alerts?
- ✓ Let you reliably turn on the P in WIPS?
- ✓ Automate BYOD policy enforcement and onboarding?
- ✓ Accurately track physical location of detected Wi-Fi devices?
- ✓ Do all of the above without compromising on Wi-Fi access features and ripping off your IT budget?

# Thank You!



## Cloud Managed Secure Wi-Fi Solutions

### **Tom Haak**

Director Sales

Konrad-Zuse-Platz 8  
81829 Munich  
Germany

P. +49 89 207042400  
M. +49 179 2414200  
E. [tom.haak@airtightnetworks.com](mailto:tom.haak@airtightnetworks.com)

### **Leo Sterr**

Senior Sales Engineer

Konrad-Zuse-Platz 8  
81829 Munich  
Germany

P. +49 89 207042401  
M. +49 151 12197767  
E. [leo.sterr@airtightnetworks.com](mailto:leo.sterr@airtightnetworks.com)